

~~CONFIDENTIAL~~

27 JAN 1983

MEMORANDUM FOR: Chairman, Computer Security Subcommittee

FROM: 

CIA Member

SUBJECT: DCID - Recommended Changes (U)

These are my suggested revisions.

Page 2, Para 1, Line 2 - one or two members vs two or more.Page 2, Para 2, Line 4 - change may to should.Page 2, Para 2, Line 5/6 - change preengineered to logical.Page 2, Para 2, Line 6 - change - will be allowed/required to may forced.Next Line - change - may to could.Page 2, under AUTHORITY, Last Para, Line 9 - period after Authority, delete and - capitalize All.

Page 3, under EXEMPTIONS (see basic contradiction) add following at end of para - No exception shall be granted which allow personnel with less than a TOP SECRET clearance based on a background investigation to access an ADP system or network which contains Sensitive Compartmented Information (SCI).

*data in*

Page 5, Para I.2.a., Line 2 - change - foreign intelligence and counter intelligence to intelligence information - this change should be carried throughout the paper - see foot note #2 on page 1.

Same Para - change - Discretionary to Need-to-know.

Page 6, Para I.2.b. - omit last sentence - the paper grants exemptions in the introduction, so why mention it again.

Same Page, Para I.2.b(2). (how about protection of sources and methods) - omit para since changing discretionary to need-to-know needs no explanation.

~~CONFIDENTIAL~~

CONFIDENTIAL

Page 8, II.1.a. - report to who; provide to who?

Page 8 - omit Section II.2., Personnel Security - this is covered under each mode in later paras.

Page 10, Para II.8. - omit - see foot note #3 front page.

Page 11, Line 7 - omit sentence beginning with They and ending with environments.

Page 12, Para III.1.f. ("approved manner" - explain) last sentence - delete TOP SECRET and Sensitive Compartmented Information - intelligence information, including SECRET, warrants a controlled copy of the operating system.

Same Page, Para III.1.g. - include core and temporary memory overwrite.

Same Page, Para III.2.b(1) - change discretionary to need-to-know.

Same Para, Sec.(3) - add after media - Any automated system presently operating which is not capable of satisfying this requirement need not be retrofitted; however, stringent controls must be exercised to assure that security labels are identified with the data recorded on the media.

Page 13, Para III.2.g. - include core and temporary memory overwrite.

Page 13, Para III.3.b(2) - change - discretionary to need-to-know.

Page 14, Line 2 - change are to is.

Page 15, Para III.4. - is not Expanded Compartmented Mode the same as Multi-level?

Page 15, Para x.2.d(2) (?) - change to III.4.b.

→ Same Para, Sec.(2) - change to read - be capable of enforcing need-to-know access control on a per-user basis and the principle of least privilege should pervade throughout system operations.

Page 16, - add to para 1 - All secret cleared users must be auditable both for access to the system and the information they process and retrieve.

Same Page, Para (5), Line 2 - change are to is.

CONFIDENTIAL

~~CONFIDENTIAL~~

Same Page, Para III.4.c(1) - insert before only - Prior to the start of operations in the Expanded Compartmented Mode, The system must be tested and validated to assure the above minimum requirements are in effect and functioning as prescribed. The system manager and the ISSO must certify the system to the NFIB member before accreditation takes effect.

Page 17, Para III.4.f(2) - need guarantees against library viewing, core viewing, relational data base segregation and internal spillage.

Page 17, add Para III.5. - titled - Exemptions.

Same Page, add Para III.5.a. - No exemptions or exceptions will be granted under the requirements stated above when operating in the Expanded Compartmented Mode. (U)

GENERAL OBSERVATIONS:

1. More mapping of A/B system specs needed for ECM: see suggestions (U)
2. Responsible authority should have prerogative to except certain SCI data from ECM. (U)

25X1



~~CONFIDENTIAL~~